State of West Virginia Office of Technology
Policy: Acceptable Use of Portable Devices
Issued by the CTO

1.0 PURPOSE

Portable devices provide mobility, flexibility, and convenience for State employees. They also offer an elevated risk of infection from viruses when connected to less secure networks, and therefore require higher standards of accountability than desktop devices.

State employees are provided the use of State-owned portable devices on an as-needed basis to access the State network, or to conduct State business from a remote location, except as specified within this document.

The purpose of this policy is to establish and communicate acceptable use, security, and confidentiality requirements related to the use of State-owned portable devices within all sites connected to and supported by the State's network infrastructure.

The term *portable device* as used in this document includes: laptops, flash drives, notebooks, personal digital assistants (PDAs), SmartPhone (e.g.: Blackberry, Treo, etc.), tablet PCs, and any emerging technology containing a processor and/or memory. The security safeguards may vary by device type, but in all cases must comply with the requirements set forth in this policy. This document is not all-inclusive and management has the authority and discretion to appropriately address any unacceptable behavior and/or practice not specifically mentioned herein.

2.0 SCOPE

This policy applies to all State employees who use State-owned and authorized portable devices.

3.0 BACKGROUND

Under the provisions of West Virginia Code §5A-6-4a, the Chief Technology Officer is granted both the authority and the responsibility to develop information technology (IT) policy, promulgate that policy, audit for policy compliance, and require corrective action where compliance is found to be unsatisfactory or absent. The

Governor's Executive Order No. 6-06, signed on August 16, 2006, empowers the CTO to "issue information security policies applicable to all Executive Branch department-level organizations."

This policy is one in a series of IT related policies intended to define and enable the incorporation of appropriate practices into all activities using technology in the State of West Virginia.

4.0 RELEVANT DOCUMENTS/MATERIAL

4.1 West Virginia Office of Technology (WVOT)

4.2 WVOT - IT Security Web Page

4.3 WVOT Policies Issued by the Chief Technology Officer (CTO)

4.4 Procedure WVOT-PR1004-Security for State-owned Portable Devices

4.5 WVOT - State of West Virginia Information Security Policy

4.6 West Virginia Code §5A-6-4a – "Duties of the Chief Technology Officer Relating to Security of Government Information"

4.7 Governor's Executive Order No. 6-06

5.0 RESPONSIBILITY/REQUIREMENTS

5.1 Employee Responsibilities

5.1.1 Employees using portable devices must exercise care to safeguard their devices from loss or theft as specified in WVOT-PR1004 – *Security for State-Owned Portable Devices*.

5.1.2 Employees are only permitted to use State-issued portable devices for State business objectives.

5.1.3 Only minimal personal use of State-provided IT resources is permitted, and should not interfere with the legitimate business of the State. (See WVOT-PO1001 – *State of West Virginia Information Security Policy, Appendix A*)

5.1.4 Each employee must ensure that the portable device receives all available program updates, security patches, and anti-virus updates at designated intervals, as specified in section 4.1.1.1 of WVOT-PR1004. If assistance is required, it should be arranged through the WVOT Service Desk.

5.1.4.1 In order to receive updates each portable device must be connected and logged-on to the State network unless it has an alternate update mechanism used within its design.

5.1.4.2 Employees must not uninstall or de-activate any security content loaded onto the mobile device by the West Virginia Office of Technology (WVOT).

5.1.4.3 The WVOT reserves the right to refuse network connection for any portable device when not in compliance with this policy. The network connection will be re-enabled only after the WVOT verifies the security status to be in compliance.

5.1.5 For security purposes, employees must store all State data on a server (e.g., Q: and S: drives, etc.).

5.2 Data Confidentiality

5.2.1 Password protection for a given device may not offer adequate protection for all data stored on the device; therefore, all portable devices must be encrypted, if technically possible. Highly sensitive data must be safeguarded to a standard that reflects due care. The method of encryption will be compliant with WVOT standards, as well as installed and configured by the appropriate WVOT technician or designated individual.

5.2.2 Employees must take every precaution to ensure the privacy of information (See WVOT-PR1004 for more information).

5.2.3 Due to the vulnerability of encryption keys remaining in computer memory, hibernation and stand-by modes should not be utilized when a device is in an unsecured location.

5.3 Security Requirements

5.3.1 All portable devices must have password functionality enabled, and encryption installed and enabled, if available.

5.3.2 Upon installation, WVOT technicians, or trained Points of Contact (POCs), e.g. Equipment Coordinators (EC will install anti-virus software onto each portable device, if applicable. Employees must not defeat any process to update virus signatures or other security system.

5.3.3 Upon installation, each portable device, where applicable, will be joined to the State domain or equivalent secure Group Policy Active Directory domain by an appropriate technician.

5.3.4 Each portable device must use a firewall, if available. Settings will be the most restrictive possible, while also allowing acceptable use of the device.

5.4 Flash Drives

5.4.1 Flash drives are for temporary data storage only, and may be used to transport State business data. Employees must not use flash drives for long term data storage.

5.4.2 If a State network connection is unavailable (e.g., off-site use), flash drives may be used for short term data storage to maintain a copy of the data until a network is available, and more secure storage is accessible on State-provided PCs, laptops, tablets, etc.

5.4.3 Employees must only use flash drives with WVOT-approved password and encryption capability to store State information.

5.4.4 Employees are prohibited from using flash drives or media that do not have adequate protection mechanisms to store or transmit sensitive data (e.g., Protected Health Information {PHI} or Personally Identifiable Information {PII}).

5.4.5 Employees must **not** connect unapproved flash drives to any State-owned computing device prior to scanning the drive for the presence of malicious code, or copy State data onto an unapproved flash drive.

5.4.6 Agencies may prohibit flash drive use at any time in order to protect data or to protect the data on systems. This prohibition should be implemented through policy, training, and/or use of technical controls (e.g. port blocking).

5.5 Physical Care

5.5.1 In all cases, manufacturer's guidelines for the care and safety of portable devices must be followed. (For more information, see WVOT-PR1004 - *Security for State-owned Portable Devices*)

6.0 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action up to, and including, dismissal. Disciplinary action, if determined to be necessary, will be administered by the employing agency and may be based on recommendations of the WVOT and the West Virginia Division of Personnel, intended to address severity of the violation and the consistency of sanctions.

7.0 DEFINITIONS

7.1 Chief Technology Officer (CTO) – The person responsible for the State's information resources.

7.2 Confidential Data – Information that is legally protected (e.g: Protected Health Information) or otherwise deemed by a qualified expert to be unsuitable for open access.

7.3 Contractor – Anyone who has a contract with the State or one of its entities.

7.4 Employee – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of Information Technology and Security policy, the term "employee" shall include the following: contractors, subcontractors, contractors' employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the WVOT to be subject to this policy. This definition does not create any additional rights or duties.

7.5 Flash Drive – A small memory drive that connects to a computer directly through a USB port. (Also known as thumb drive.)

7.6 Firewall – A network node set up as a boundary to prevent traffic from one segment to cross over to another. Firewalls are used to improve network traffic, as well as for security purposes.

7.7 Information Security Administrator (ISA) – The person designated by the agency head to assure the agency's compliance with State Information Security policies and procedures. The ISA is the agency's internal and external point of contact for all Information Security matters.

7.8 Personal Digital Assistant (PDA) – A handheld device that combines computing, telephone/fax, and networking features. A typical PDA can function as a cellular phone, fax sender, and personal organizer.

7.9 Personally Identifiable Information (PII) – Includes all protected and non-protected information that identifies, or can be used to identify, locate, or contact an individual.

7.10 Points of Contact (POC) – Technical Points of Contact and/or Equipment A master listing is maintained by WVOT User Management.

7.11 Portable Devices– Includes laptops, notebooks, flash drives, PDAs, Smart phones, tablet PCs, and any emerging technology containing a processor and/or memory.

7.12 Protected Health Information (PHI) – Health information transmitted by or maintained in electronic media used to identify an individual, which is created, used, or disclosed in the course of providing health care services such as diagnosis or treatment. Examples include: names, phone numbers, medical record numbers, photos, etc.

7.13 SmartPhone – A wireless handheld device that supports e-mail, mobile telephone, text messaging, web browsing and other wireless information services. (e.g: Blackberry, Treo, etc.)

7.14 West Virginia Division of Personnel – The division of the Department of Administration established by West Virginia Code § 29-6-1 *et seq.*, which is responsible for the system of human resource management for operating agencies in the classified and classified-exempt service of West Virginia State government.

7.15 West Virginia Office of Technology (WVOT) - The division of the Department of Administration established by WV Code § 5A-6-4a, et. seq., which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.

8.0 LEGAL AUTHORITY

The CTO is charged with securing State government information and the data communications infrastructure from unauthorized uses, intrusions, or other security threats. The CTO has authority to issue policies, procedures, and standards to accomplish this mission. This policy will apply across the Executive Branch, with the exclusion of the West Virginia State Police, the Division of Homeland Security and

Emergency Management, any constitutional officers, the West Virginia Board of Education, the West Virginia Department of Education, and the county boards of education. To the extent that there are policies in place which provide less security than this policy, they will be superseded by this policy. In instances where existing state and federal laws and regulations are more restrictive than Information Security policies issued by the WVOT, the more restrictive provisions will prevail.

9.0 INDEX